(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年2 月17 日 (17.02.2005)

PCT

(10) 国際公開番号
WO 2005/015419 A1

(51) 国際特許分類[7]: G06F 15/00, H04L 12/28

(21) 国際出願番号: PCT/JP2004/011475

(22) 国際出願日: 2004 年8 月10 日 (10.08.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-291971 2003 年8 月12 日 (12.08.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 嶋 久登 (SHIMA, Hisato) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 中野 雄彦 (NAKANO, Takehiko) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

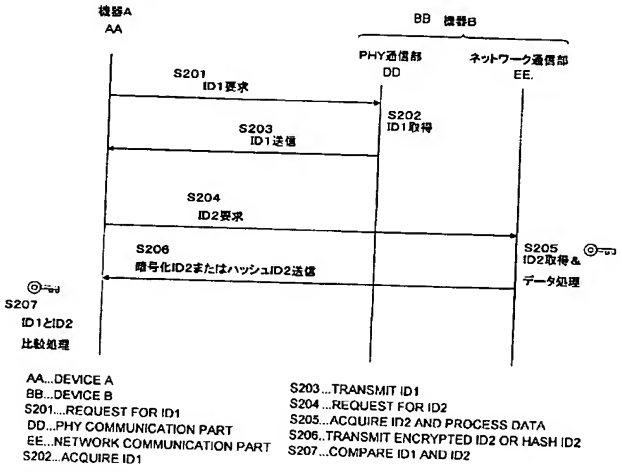
(74) 代理人: 宮田 正昭, 外(MIYATA, Masaaki et al.); 〒1040041 東京都中央区新富一丁目１番７号 銀座ティーケイビル 澤田・宮田・山田特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: COMMUNICATION PROCESSING APPARATUS, COMMUNICATION CONTROL METHOD, AND COMPUTER PROGRAM

(54) 発明の名称: 通信処理装置、および通信制御方法、並びにコンピュータ・プログラム



(57) Abstract: An arrangement capable for preventing secret information, such as private data and contents that are copyrighted or whose utilizations are limited, in a local network from being leaked or distributed outside the local network. A plurality of identification information of a communication destination device are acquired at different data processing levels. For example, identification information acquired by a data processing in a physical layer or data link layer level in an OSI reference model and identification information acquired by a data processing in a layer level higher than a network layer level are received and compared. As at least one of such identification information, data produced by an encryption processing based on secret information shared with a communication source device or data produced by hash values shared with the communication source device is received. In this way, the plurality of identification information are compared, and it is determined, based on the comparison result, whether the communication destination device is a device connected to the same local network.

[続葉有]

WO 2005/015419 A1

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: ローカルネットワーク内の秘密情報、例えば私的データや、著作権、利用権の制限されたコンテンツの外部に対する漏洩、流出を未然に防止することを可能とした構成を提供する。通信先デバイスの識別情報を異なるデータ処理レベルで複数取得する。例えばＯＳＩ参照モデルにおける物理層またはデータリンク層レベルにおけるデータ処理によって取得した識別情報と、ネットワーク層以上の層レベルにおけるデータ処理によって取得した識別情報とを受信し、これらの識別情報の照合を行う。また、少なくとも１つの識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成による生成データを受信する。複数の識別情報の照合を行い、照合の成立または非成立に基づいて、通信先デバイスが同一のローカルネットワークに接続されたデバイスであるか否かを判定する。

明 細 書

通信処理装置、および通信制御方法、並びにコンピュータ・プログラム

技術分野

[0001] 本発明は、通信処理装置、および通信制御方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、例えばホーム・ネットワーク等のローカルネットワーク内に接続された機器と、インターネット等の外部ネットワークに接続されけた機器とを区別可能とした認証を実行して通信を行うことにより、例えばホーム・ネットワーク内でのみ利用の許容されたコンテンツの外部流出など、コンテンツ不正利用処理などを排除可能とした通信処理装置、および通信制御方法、並びにコンピュータ・プログラムに関する。

背景技術

[0002] 昨今のデータ通信ネットワークの普及に伴い、家庭内においても家電機器やコンピュータ、その他の周辺機器をネットワーク接続し、各機器間での通信を可能とした、いわゆるホーム・ネットワークが浸透しつつある。ホーム・ネットワークは、ネットワーク接続機器間で通信を行なうことにより各機器のデータ処理機能を共有したり、機器間でコンテンツの送受信を行なう等、ユーザに利便性・快適性を提供するものであり、今後、ますます普及することが予測される。

[0003] しかし、一方、この種のネットワークでは、不正アクセスに対する対策を考慮することも必要となる。ホーム・ネットワーク内の機器、例えばサーバ等には私的なコンテンツや有料コンテンツ等の著作権管理を要求されるコンテンツが格納されることも多い。

[0004] このようなホーム・ネットワーク内のサーバに格納されたコンテンツや秘密情報は、例えば、インターネットを介した外部からのアクセスによって不正に取得される可能性がある。このような不正アクセスを許容すると、秘密漏洩を生じさせることにもなり、また、コンテンツ著作権の管理の観点からも重要な問題である。

[0005] このように、映画や音楽など著作権の管理が必要なコンテンツをネットワークを通じて伝送する場合、そのコンテンツ伝送範囲は利用が許可された範囲、例えばホーム・ネットワーク内のデバイス間に留めることが求められるが、近年のインターネットの普

及に伴い、インターネットを介したコンテンツの不正な伝送が行われ、問題になっている。

[0006] 著作権法の下、デジタル・コンテンツは著作物の1つとして、無断の複製や改竄などの不正使用から保護を受ける。著作権法第30条では、著作物の種類や複製の態様を限定することなく、個人的に又は家庭内などで使用する目的であれば、使用する者本人が複製することができることとされている。また、同法第49条第1項においては、私的使用のために作成した複製物をその目的以外のために使用した場合には著作権者の複製権が動く旨を規定し、いわゆる目的外使用を禁止している。

[0007] デジタル・コンテンツの利用が盛んな今日においては、その著作権保護を目的とした多くの技術が開発されている。例えば、デジタル伝送コンテンツの保護に関する業界標準であるDTCP(Digital Transmission Content Protection)では、著作権が保護された形でコンテンツを伝送させるための仕組みについて規定している。例えば、非特許文献1[DTCP Specification Volume 1 Version 1.3 (Informational Version)http://www.dtcp.com/data/info_20040107_dtcp_Vol_1_1p3.pdf]を参照のこと。

[0008] DTCPは、IEEE1394などを伝送路に用いたホーム・ネットワーク上におけるデジタル・コンテンツの伝送について規定している。ホーム・ネットワーク経由でのコンテンツ伝送は、著作権法で言うところの個人的又は家庭の範囲内での使用であると推定される。DTCPでは、コンテンツ伝送時における機器間の認証プロトコルと、暗号化コンテンツの伝送プロトコルについて取り決めている。

[0009] すなわち、コンテンツ提供元であるサーバは、コンテンツ提供先であるクライアントと認証を行ない、この認証手続きを経て共有化される鍵を用いて伝送路を暗号化し、コンテンツの伝送を行なう。したがって、DTCPによればコンテンツを保護しながら伝送することができる。また、クライアントは、サーバとの認証に成功しないと暗号鍵を取得できないから、コンテンツを享受することはできない。

非特許文献1:DTCP Specification Volume 1 Version 1.3 (Informational Version)http://www.dtcp.com/data/info_20040107_dtcp_Vol_1_1p3.pdf

発明の開示

発明が解決しようとする課題

[0010] 本発明は、このような状況に鑑みてなされたものであり、ホーム・ネットワーク等の特定のローカルネットワーク内の機器と、インターネット等の外部ネットワークに接続された機器とを明確に区別する認証構成を実現したものである。コンテンツ等のデータ転送の際には、認証処理を実行し、ホーム・ネットワーク等のローカルネットワークの接続機器であることの確認を行う構成とすることで、コンテンツの不正流出、秘密情報の漏洩等の防止を可能とした通信処理装置、および通信制御方法、並びにコンピュータ・プログラムを提供することを目的とする。

課題を解決するための手段

[0011] 本発明の第1の側面は、

ネットワークを介した通信処理を実行する通信処理装置であり、

所定の認証方式に対応したローカルネットワーク内の機器にのみ開示が許可されている秘密情報を取得するため、前記認証方式による認証処理に関連した通信処理を行い、

OSI参照モデルにおけるネットワーク層以下のデータ処理によって、前記通信処理における通信先デバイスの固有識別情報を取得し、

OSI参照モデルにおけるアプリケーション層のデータ処理として、前記認証方式の認証シーケンスにて、認証相手デバイスの固有識別情報を取得し、

取得した、前記通信先デバイスの固有識別情報識別情報と、前記認証相手デバイスの固有識別情報との照合を行い、

該照合の成立または非成立に基づいて、認証相手デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する構成を有することを特徴とする通信処理装置にある。

[0012] さらに、本発明の通信処理装置の一実施態様において、通信先デバイスから受信する少なくとも1つの固有識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成処理によって生成した処理データとして受信する構

成であることを特徴とする。

[0013] さらに、本発明の通信処理装置の一実施態様において、通信先デバイスから受信する識別情報は、IEEE1394規格によって規定されたノードユニークIDであることを特徴とする。

[0014] さらに、本発明の通信処理装置の一実施態様において、前記通信処理装置は、通信先デバイスから受信する識別情報として、通信先デバイスのPHY通信部の取得した識別情報と、通信先デバイスのネットワーク通信部の取得した識別情報とを受信し、これらの複数の識別情報の照合を行う構成であることを特徴とする。

[0015] さらに、本発明の通信処理装置の一実施態様において、通信先デバイスから受信する識別情報は、通信規格によって規定されたデバイス・アドレスであることを特徴とする。

[0016] さらに、本発明の通信処理装置の一実施態様において、前記通信処理装置は、通信先デバイスから受信する識別情報として、通信先デバイスの送信するパケットのソースアドレスとしてのデバイス・アドレスと、アプリケーションレベルにおけるデータ処理によってパケットに格納したデバイス・アドレスまたはデバイス・アドレスに基づくデータを受信し、これらの複数のデバイス・アドレスの照合を行う構成であることを特徴とする。

[0017] さらに、本発明の第2の側面は、

ネットワークを介した通信処理を実行する通信制御方法であり、

OSI参照モデルにおけるネットワーク層以下のデータ処理によって、通信処理における通信先デバイスの固有識別情報を取得し、OSI参照モデルにおけるアプリケーション層のデータ処理として、所定の認証方式の認証シーケンスにて、認証相手デバイスの固有識別情報を取得する識別情報取得ステップと、

取得した、前記通信先デバイスの固有識別情報識別情報と、前記認証相手デバイスの固有識別情報との照合を実行する照合処理ステップと、

該照合の成立または非成立に基づいて、認証相手デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する判定ステップと、

を有することを特徴とする通信制御方法にある。

[0018] さらに、本発明の通信制御方法の一実施態様において、前記識別情報取得ステップにおいて通信先デバイスから受信する少なくとも1つの固有識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成処理によって生成した処理データとして受信することを特徴とする。

[0019] さらに、本発明の通信制御方法の一実施態様において、通信先デバイスから受信する識別情報は、IEEE1394規格によって規定されたノードユニークIDであることを特徴とする。

[0020] さらに、本発明の通信制御方法の一実施態様において、前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、通信先デバイスのPHY通信部の取得した識別情報と、通信先デバイスのネットワーク通信部の取得した識別情報とを受信するステップであり、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする。

[0021] さらに、本発明の通信制御方法の一実施態様において、通信先デバイスから受信する識別情報は、通信規格によって規定されたデバイス・アドレスであることを特徴とする。

[0022] さらに、本発明の通信制御方法の一実施態様において、前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、通信先デバイスの送信するパケットのソースアドレスとしてのデバイス・アドレスと、アプリケーションレベルにおけるデータ処理によってパケットに格納したデバイス・アドレスまたはデバイス・アドレスに基づくデータを受信し、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする。

[0023] さらに、本発明の第3の側面は、

ネットワークを介した通信処理を実行するコンピュータ・プログラムであり、

OSI参照モデルにおけるネットワーク層以下のデータ処理によって、通信処理における通信先デバイスの固有識別情報を取得し、OSI参照モデルにおけるアプリケーション層のデータ処理として、所定の認証方式の認証シーケンスにて、認証相手デバイスの固有識別情報を取得する識別情報取得ステップと、

取得した、前記通信先デバイスの固有識別情報識別情報と、前記認証相手デバイスの固有識別情報との照合を実行する照合処理ステップと、

該照合の成立または非成立に基づいて、認証相手デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する判定ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

[0024] なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

[0025] 本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

発明の効果

[0026] 本発明の構成によれば、ホーム・ネットワーク等のネットワークに対して、インターネット等の外部ネットワークに接続された機器からアクセスされた場合、そのアクセスが外部機器からか内部のローカルネットワーク内の機器からであるかを明確に判別することが可能となり、本発明の判定を伴う認証を実行することによりローカルネットワーク内の秘密情報、例えば私的データや、著作権、利用権の制限されたコンテンツの漏洩、流出を未然に防止することが可能となる。

[0027] 本発明の構成では、通信先デバイスの識別情報を異なるデータ処理レベルで複数取得する。例えば少なくとも1つの識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成処理によって生成した処理データとして受信する。また、OSI参照モデルにおける物理層またはデータリンク層レベルにおけるデータ処理によって取得した識別情報と、ネットワーク層以上の層レベルにおけるデ

ータ処理によって取得した識別情報とを受信し、これらの複数の識別情報の照合を行う。このように、複数の異なるデータ処理レベルで取得された識別情報の照合を行い、照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かが確実に判定され、ローカルネットワーク内の秘密情報、例えば私的データや、著作権、利用権の制限されたコンテンツの外部に対する漏洩、流出を未然に防止することが可能となる。

[0028] 本発明の構成によれば、IEEE1394規格におけるノードユニークIDや、ブルートゥース規格におけるブルートゥースデバイス・アドレスを適用した比較照合が可能であり、既存の通信において設定済みの識別情報を利用可能となる。

発明を実施するための最良の形態

[0029] 以下、図面を参照しながら本発明の通信処理装置、および通信制御方法、並びにコンピュータ・プログラムの詳細について説明する。

[0030] まず、図1を参照して、本発明の適用可能なネットワーク構成例について説明する。図1は、例えば特定ユーザの家等に構築されたホーム・ネットワーク100等のローカルエリアネットワーク、すなわち内部ネットワークであり、パーソナルコンピュータ(PC)101、102、TV103、ハードディスクレコーダ104、PDA105等の様々な情報処理装置がホーム・ネットワーク100を介してデータ送受信を行う。

[0031] たとえば、PC101、102、あるいはハードディスクレコーダ104をコンテンツ提供サーバとし、TV103、PDA105をクライアントとして、クライアントがサーバの格納コンテンツをネットワークを介して取得し、クライアントのディスプレイ、スピーカを利用してコンテンツ出力を行う。

[0032] ホーム・ネットワーク100は、有線、無線等いずれかのネットワークであり、各接続機器は、通信パケットをネットワークを介して送受信する。

[0033] 図1において、ホーム・ネットワーク100は、インターネット等の外部ネットワーク120に接続されている。外部ネットワーク120にもPC121、携帯電話122、ポータブル再生プレーヤ123等の各種の通信処理装置が接続される。ホーム・ネットワーク100内の通信処理装置と外部ネットワーク120の通信処理装置とは、外部ネットワーク120

およびホーム・ネットワーク100を介して通信が可能となる。

[0034] 外部ネットワーク120およびホーム・ネットワーク100によって構成される内部ネットワークの間には、外部ネットワーク120と内部ネットワーク間の通信を可能とするデータ処理、例えばホーム・ネットワーク内のデータ通信パケットであるIEEE1394パケットと、外部ネットワークでの転送パケットであるイーサネットパケット、IPパケットの変換などを実行する通信サーバ110が接続される。

[0035] 従来のように、機器同士の認証が成功すればコンテンツ取得が可能となるシステムにおいては、外部ネットワーク120に接続されたPC121、携帯電話122、ポータブル再生プレーヤ123等の各種の通信処理装置は、通信サーバ110を介してホーム・ネットワーク100内のサーバ、例えばPC101、102、ハードディスクレコーダ103等にアクセスし、これらの装置に格納されたコンテンツを取得してPC121、携帯端末122、再生プレーヤ123等においてコンテンツ出力を行うことが可能となる。

[0036] ただし、これらのコンテンツ取得を不特定のクライアントに許容することは、コンテンツの著作権、秘密漏洩等の問題から好ましいことではない。従って、機器間の通信においては、後段で説明する本発明の認証シーケンスに従った認証処理を実行し、内部ネットワーク内のデータが外部に不正に流出するのを防止する構成としている。この詳細処理構成については後述する。

[0037] 図1に示す各ネットワーク接続機器としての通信処理装置のハードウェア構成例について図2を参照して説明する。

[0038] CPU(Central Processing Unit)201は、ROM(Read Only Memory)202、またはHDD(Hard Disk Drive)204等に記憶されているプログラムに従って、各種の処理を実行し、データ処理手段、あるいは通信制御処理手段として機能する。RAM(Random Access Memory)203には、CPU201が実行するプログラムやデータが適宜記憶される。CPU201、ROM202、およびRAM203、HDD204は、バス205を介して相互に接続されている。

[0039] バス205には、入出力インタフェース206が接続されており、この入出力インタフェース206には、例えば、ユーザにより操作されるキーボード、スイッチ、ボタン、あるいはマウス等により構成される入力部207、ユーザに各種の情報を提示するLCD、CR

T、スピーカ等により構成される出力部208が接続される。さらに、データ送受信手段として機能する通信部209、さらに、磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリなどのリムーバブル記録媒体211を装着可能で、これらのリムーバブル記録媒体211からのデータ読み出しあるいは書き込み処理を実行するドライブ210が接続される。通信部209は、例えばIEEE1394規格に従った通信、あるいはブルートゥース規格に従った通信処理の可能な構成を持つ。

[0040] なお、図2に示す構成は、図1に示すネットワーク接続機器の一例としての一般的なPCの構成を示すものであるが、ネットワーク接続機器はPCに限らず、図1に示すように携帯電話、PDA等の携帯通信端末、その他の様々な電子機器、通信処理装置によって構成することが可能である。従って、それぞれの機器固有のハードウェア構成を持つことが可能であり、そのハードウェアに従った処理を実行する。

[0041] 本発明の通信処理装置において実行する機器間の通信においては、まず機器間の認証処理を実行し、認証処理の結果、通信相手が同一のホーム・ネットワーク等のローカルネットワーク接続された機器であることが確認された場合に、コンテンツ等のデータ転送を許容する。認証処理においては、通信先デバイスを一意に識別できる固有の識別情報を複数の異なるデータ処理レベルで取得し、取得した複数の識別情報の照合を行い、該照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する。

[0042] 1つの具体例としては、例えば通信機器の識別子(ID)をOSI参照モデルにおける物理層やデータリンク層での通信と、ネットワーク層以上の例えばアプリケーション層での通信においてそれぞれ受領し、この2つのIDを比較する処理を行う。以下、本発明に従った認証処理の具体例について、IEEE1394規格に従った通信を行う構成例と、ブルートゥース規格に従った通信を行う構成例について説明する。

[0043] (1)IEEE1394規格に従った通信を行う構成例

ホーム・ネットワーク等のローカルネットワークに接続された通信処理装置は、IEEE1394データインターフェイスを備え、IEEE1394方式に従ったデータ転送を実行する。IEEE1394データインターフェイスは、例えばSCSIなどよりもデータ転送レート

が高速であり、所要のデータサイズを周期的に送受信することが保証されるアイソクロナス(Isochronous)通信が可能である。このため、IEEE1394データインターフェイスは、AV(Audio/Video)などのストリームデータをリアルタイムで転送するのに有利となる。

[0044] IEEE1394によるデータ伝送方式には、上述のアイソクロナス(Isochronous)通信方式と、非同期で通信するアシンクロナス(Asynchronous)通信方式が存在する。一般に、アイソクロナス(Isochronous)通信方式はデータの送受信に用いられ、アシンクロナス(Asynchronous)通信方式は各種制御コマンドの送受信に用いられる。1本のケーブルを使用して、これら2種類の通信方式によって送受信を行うことができる。

[0045] 各種デジタルAV機器やパーソナルコンピュータ装置等の電子機器を、IEEE(Institute of Electrical Engineers)1394等のデジタルデータインターフェイス規格に従ったデータバスを介して相互に接続することで、機器間でデータを送受信できるようにしたデータ伝送システムが構築される。

[0046] このようなAVシステムでは、いわゆるリモート制御も可能となる。例えば、データバスを介してディスク記録再生装置とパーソナルコンピュータが接続されると、ディスク記録再生装置に対する記録再生、更には記録ソースの編集などに関する操作をパーソナルコンピュータ装置側での操作によって行うことも可能となる。

[0047] 本発明の通信処理装置としてのIEEE1394対応機器の構成について図3を用いて説明する。

[0048] 送受信部301の内部には、データ処理手段としてPHY−IC303、LINK−IC304、ネットワーク通信部(IEEE1394制御マイコン)305を有する。なお、PHY−IC303とLINK−IC304をまとめてPHY通信部とみなす。

[0049] PHY−IC303は、物理層の電気的インタフェースを受け持ち、LINK−IC304からのデータを変換し、IEEE1394規格の電気信号を発生し、逆にIEEE1394規格信号をLINK−IC304に送信する。また、PHY−IC303は、バス(ケーブル)の状態認識、バスの初期化、アービトレーション処理などを実行する。すなわち、PHY−IC303は、IEEE1394規格のプロトコルに従って、IEEE1394端子302を介してIEEEシ

リアルバス310との間の通信を制御し、IEEE1394シリアルバス310から供給されるデジタルビデオデータやデジタルオーディオデータがパケット化されたアイソクロナスパケット、または制御信号がパケット化されたアシンクロナスパケットをLINK−IC304に供給する。PHY−IC303はまた、LINK−IC304から供給されるアイソクロナスパケットやアシンクロナスパケットを、IEEE1394シリアルバス310に出力する。

[0050] LINK−IC304は、データリンク層を受け持ち、送信データパケットのPHY−IC303への送出、PHY−IC303受信パケットのトランザクション／アプリケーション層への送出を実行する。すなわち、PHY−IC303から供給されるアシンクロナスパケットを、IEEE1394制御マイコン305が解読できるデジタル信号（コマンド）に変換し、IEEE1394制御マイコン305に供給したり、IEEE1394制御マイコン305から供給されるデジタル信号をアシンクロナスパケットに変換し、PHY−IC303に供給する。LINK−IC304はまた、PHY−IC303から供給されるアイソクロナスパケットをデジタル信号に変換したり、機器から入力される主データ（例えば、デジタルビデオデータ、デジタルオーディオデータ）を、アイソクロナスパケットに変換し、PHY−IC303に供給する。

[0051] ネットワーク通信部（IEEE1394制御マイコン）305は、LINK−IC304から供給されたコマンドを機器制御マイコン306に転送するとともに、そのコマンドに対応するレスポンスを生成し、LINK−IC304に出力する。

[0052] 機器制御マイコン306は、ネットワーク通信部（IEEE1394制御マイコン）305から供給されたコマンドに対応して、機器内部の回路（図示せず）を制御し、各種の処理を実行させる。

[0053] LINK−IC304は、EPROMなどのメモリ321が接続ないし内蔵され、メモリ321に書き込まれたIDを読み取ることができる。図では、メモリ321をLINK−IC304に内蔵した例を示している。

[0054] メモリ321に格納されるIDは、IEEE1394バス上の各ノードでグローバルユニーク（Global Unique）な値を用いるものとする。以降、このIDをNUID（Node Unique ID）と呼ぶ。また、LINK−IC304、メモリ321は、耐タンパ構成を持つパッケージとして構成され、IDや通信内容の改ざんの困難性を高めた構成を持つ。IDの改ざんを困難にする方法の具体例としては、例えば、LINK−IC304とIDの格納メモリ321を1つの

ICで構成することや、複数のICで構成される場合はIC間の通信を保護するために通信路を暗号化したり、あるいはICをBGAパッケージにして、配線を基板の内層に埋め込んで信号にアクセスできなくするといった構成とするなどの各種構成が適用可能である。

[0055] ネットワーク通信部(IEEE1394制御マイコン)305は、LINK−IC304を通じて他のネットワーク接続機器のネットワーク通信部と通信を行うことができる。また、各ネットワーク通信部は、自身のLINK−IC304経由でNUIDを読み取ることができる。

[0056] 以上のように構成される1394対応機器は、IEEE1394シリアルバス310を介して、他の各接続機器とデータ送受信、通信を実行することができる。なお、IEEE1394バスでは機器の抜き差しなどによりバスリセットが生じ、バスリセットに伴い、バスの初期化を行う。バス初期化シーケンスにおいて、バス上の各機器に通信用のIDがアサインされる。これをノードIDと呼ぶ。アシンクロナスパケットによる通信を行う際には、パケットヘッダのパケット送信先フィールドに相手機器のノードIDを、パケット送信元フィールドに自分のノードIDを入れる。

[0057] 例えばIEEE1394対応機器としてのVTRに所定の機能を実行させるとき、IEEE1394バスに接続されたパーソナルコンピュータ(PC)は、その機能の実行を指令する、例えば、再生、記録、巻戻しなどのAV／Cコマンド(以下、これらをまとめてAV／Cコマンドと称する)を、IEEE1394シリアルバスを介してVTRに伝送する。つまり、アシンクロナスパケット送信先フィールドにVTRのノードIDを入れ、AV／Cコマンドをデータフィールドに入れて、パケットを出力する。

[0058] VTRは、AV／Cコマンドを受信すると、それに対応した処理を実行するとともに、所定のレスポンスをAV／Cコマンドの送信元である、パーソナルコンピュータ(PC)に出力する。

[0059] 図4を参照して、ネットワーク接続機器間の通信の際に実行する認証処理シーケンスについて説明する。

[0060] 図4に示すフローは機器Aが、通信を行おうとする機器Bが適切な通信相手であるかを確認し、通信の可否を制御するフローである。すなわち、機器Aは、機器Bが機器Aと同一のホーム・ネットワーク内の内部ネットワーク接続機器であるか、インターネ

ット等の外部ネットワークに接続された機器であるかを判別する。なお、ここで機器Aと機器Bは同一の認証方式に対応しており、もともと認証処理アプリケーション間での通信は成功するという前提のもとに、内部ネットワーク接続機器かどうかの判別を行うものとする。つまり、機器A、機器Bはお互いの通信に必要なID(ノードID)を知っているという前提にある。

[0061] まず、機器Aは、ステップS111において、相手機器BのPHY通信部に対するコマンドとして、ID要求コマンド1を送る。機器BのPHY通信部は、ステップS112において、ID要求を受けると、ステップS113において、PHY通信部の処理として自身のIDを読み出して、ステップS114において、機器Aに対して返送する。この処理の具体的な実現例としては、後述する、IEEE1394におけるアシンクロナス通信のReadトランザクションを用いた、コンフィグレーションROM中のNUIDの読み出しがあげられる。

[0062] 機器Aは、ステップS115において、機器BのPHY通信部からのIDを受信し、受信IDを、後の処理のために記憶しておく。以上の通信は、OSI参照モデルのデータリンク層以下で実施されるものとし、ブリッジやルーターを介さないネットワーク接続機器間の通信においてのみ可能なものとする。

[0063] 次に機器Aは、ステップS116において、機器Bのネットワーク通信部に対するコマンドとして、ID要求コマンド2を送る。機器Bのネットワーク通信部は、ステップS117において、ID要求コマンド2を受けると、機器Bのネットワーク通信部は、ステップS118において、自身のPHY通信部経由でメモリに格納されたID(NUID)を読み出して、ステップS119において機器Aに対して読み出したIDを返送する。この通信は、OSI参照モデルのネットワーク層以上で実施されるものとし、ブリッジやルーターを介した機器とも通信可能なものとする。なお、この通信で得たIDを以後、ID'とする。

[0064] この処理の具体的な実現方法としては、1394 Trade Association仕様として規定されているAV/Cコマンドを用いてNUIDのリクエストコマンドを構成することなどが考えられる。例えば、AV/Cコマンドの1つとして定義されているSecurityコマンドを用いる、IEEE1394伝送の保護システムであるDTCP規格で、その認証コマンドを拡張することで実現した場合、ID要求と応答の通信はDTCP規格に対応する機器

の認証処理部(アプリケーション)の間でやり取りされることになる。

[0065] 機器Aは、ステップS120において、機器Bのネットワーク通信部からID'を受信すると、ステップS121において、受信したID'が、先に機器BのPHY通信部から受信したIDと一致するか確認する。

[0066] 一致した場合、すなわちID=ID'が成立する場合は、ステップS122に進み、相手機器との通信を許可し、引き続く通信を行う。一方、一致しない場合、すなわちID=ID'が成立しない場合は、ステップS123に進み、以後の通信を禁止する。

[0067] 機器間の通信は、通信途上での改ざんやなりすましを防止するため、両方の機器が共有する秘密データに基づいた処理で保護された状態で行われることも考えられる。例えば暗号化したり、通信内容に対する電子署名や鍵付きハッシュ値を送るなどの手段が適用されうる。なお、暗号化や電子署名の具体的なアルゴリズムとしては、共通鍵暗号方式、公開鍵暗号方式どちらも適用されうる。

[0068] 図5に、ネットワーク通信部からのID送信の際に、特定の正当な機器のみが保持する秘密情報としての鍵を適用した暗号処理やハッシュ値生成処理によって取得IDのデータ処理を実行し、暗号化データあるいはハッシュ値としてのIDを送信する構成とした例について説明する。

[0069] 機器Aは、ステップS201において、相手機器BのPHY通信部に対するコマンドとして、ID要求コマンド1を送る。機器BのPHY通信部は、ID要求を受けると、ステップS202において、PHY通信部の処理として自身のNUIDを読み出して、ステップS203において、機器Aに対してID1として返送する。

[0070] 機器Aは、機器BのPHY通信部からのIDを受信し、受信IDを、後の処理のために記憶しておく。次に、ステップS204において、機器Bのネットワーク通信部に対するコマンドとして、ID要求コマンド2を送る。機器Bのネットワーク通信部は、ID要求コマンド2を受けると、ステップS205において、自身のPHY通信部経由でメモリに格納されたID(NUID)を読み出して、機器Aと機器Bが共有する秘密データ、すなわち暗号処理鍵やハッシュ値生成鍵を適用し、読み出したIDに対する暗号処理鍵を適用した暗号化、あるいはハッシュ値生成鍵を適用したハッシュ値生成処理を行い、生成したデータをステップS206において、ID2として機器Aに送信する。

[0071] 機器Aは、受信したID2が例えば暗号化データである場合は、機器Bと共有する鍵に基づいて復号処理を実行し、復号結果として得られたID2と先にPHY通信部から受信したID1とを照合比較する。両者が一致すれば、ID1を送信した機器とID2を送信した機器とは同一であり、PHY通信部の通信が実行可能な内部ネットワーク接続機器との通信が実行されていると判定し、その後の通信、例えばコンテンツ提供を行う。ID1とID2が一致しない場合は、ID1を送信した機器とID2を送信した機器とは同一でない。すなわち、ID1は、PHY通信部の通信が実行可能な内部ネットワーク接続機器が機器Aに提供し、ID2はインターネット等、外部ネットワークに接続された機器が機器Aに送信してきたものと判定し、不正な外部からのアクセスが行われていると判定し、その後の通信、例えばコンテンツ提供を実行することなく、通信を停止する。

[0072] また、機器Aは、受信したID2が例えばハッシュ値である場合は、先にPHY通信部から受信したID1に対して、機器Bと共有するハッシュ値生成鍵に基づいてハッシュ値を生成し、結果として得られたID1に基づくハッシュ値と、機器Bのネットワーク通信部から受信したID2に基づくハッシュ値とを照合比較する。両者が一致すれば、ID1を送信した機器とID2を送信した機器とは同一であり、PHY通信部の通信が実行可能な内部ネットワーク接続機器との通信が実行されていると判定し、その後の通信、例えばコンテンツ提供を行う。不一致の場合は、上述と同様、外部からの不正アクセスであると判定し、その後の通信、例えばコンテンツ提供を実行することなく、通信を停止する。

[0073] なお、ここまでは秘密共有鍵ベースのハッシュを用いる例で説明をしたが、PKI(公開鍵暗号)ベースの電子署名を使うこともできる。この場合、機器Bは自身のPrivate鍵を用いて電子署名を求め、先のハッシュ値の代わりとして機器Aに送り、機器Aは機器Bから得た機器BのPublic鍵を用いて電子署名の正当性を検証することになる。

[0074] 本発明の上述した認証シーケンスを実行することにより、ローカルネットワークに接続された機器と、外部ネットワーク接続機器とを区別することが可能となり、外部ネットワークを介した不正アクセスを排除することができる。

[0075] すなわち、図6(a)に示すように、ローカルバス上に接続された機器A411と機器B412があり、機器A411と機器B412がこの認証方式に対応している場合、機器A411は、上述した認証シーケンスにおいて機器B412から受信するIDはID1＝ID2となる。しかし、図6(b)に示すように、機器A421と機器C422はこの認証方式に対応しているが、機器C422は機器A421と同じローカルバス上には存在していない場合、機器A421と機器C422は機器X431と機器Y432を介して通信する。ここで、この認証方式に対応していない機器X431が機器C422になりすましたとする。つまり、機器C422があたかも機器X431の位置に存在するように見せかけるため、機器C422の通信用IDと称して、実際には機器X431のノードIDを機器A421に知らせる。すなわち機器X431は機器A421から機器C422に宛てた認証アプリケーションデータを機器Y432に送り、機器Y432はそれを機器C422に送る。機器Y432は機器C422から機器A421に宛てた認証アプリケーションデータを機器X431に送り、機器X431がそれを機器A421に送る。機器A421が外部ネットワークに接続された機器C422と接続して、上述の認証シーケンスを実行した場合、機器A421はローカル接続した機器X431のPHY通信部からID1を受信し、機器C422のネットワーク通信部からID2を受信することになる。この場合、ID1は機器X431のNUIDであり、ID2は機器C422のNUIDであるため、ID1＝ID2は成立せず、機器A421は、外部ネットワーク接続機器からのアクセスであると判定し、通信を終了することができる。

[0076] 上記のように、IEEE1394では、コンフィグレーションROMに64ビットのノードユニークID(NUID)を持つことが規定されている。このIDは、IEEE1394で規定されたアシンクロナス通信によって直接参照することができる。通常ノードユニークIDの情報は、IEEE1394のICだけで処理が完結する。一方、IEEE1394のICを実装する装置において、そのIC以外のIC、例えばCPUからIEEE1394のIC経由でノードユニークIDを読み取ることができれば、上述した直接的な参照方法以外の方法でIDを受け渡すこともできる。例えば上述したように2つの機器が共有する秘密鍵を用いた暗号化データとして送受信することができる。

[0077] IEEE1394の機器同士で、本発明の処理を実行する場合、通信相手を1394のローカルバス内の機器に限定するため、1394の10ビットのバスIDは全ビット1とし、ブ

リッジを経由した異なるバス上の機器とは通信を行わないことを前提とする。

[0078] しかし、先に説明した図6(b)のように、機器X431が機器C422に、また機器Y432が機器A421になりすますことで、AV／Cコマンドなどを使うアプリケーションプロトコルはローカルバスを越えた通信を行うことも可能である。これを防ぐために機器A421は、ローカルバス内の通信相手のコンフィグレーションROMにアクセスし、ノードユニークID(NUID)を直接参照するとともに、前述のアプリケーションプロトコルによってもNUIDを取得する。この場合、機器A421は、ローカルバス上にいる機器X431のコンフィグレーションROMを参照することしかできず、機器X431のノードユニークID(NUID)を参照する一方、機器A421と共有秘密をベースとした通信をする機器は、機器C422なので、機器X431，Y432経由で機器C422のNUIDを取得することになる。これらのIDは一致しないことになり、結果として機器A421は、機器C422がローカルバス上に存在しないことを検知し、中継された通信を防止することができる。

[0079] (2)ブルートゥース規格に従った通信を行う構成例

次に、ホーム・ネットワーク等のローカルネットワークに接続された通信処理装置が、ブルートゥース規格に従った通信を行う構成例について説明する。

[0080] 近年、近距離間の無線通信手段としてブルートゥース(Bluetooth)が注目されており、様々な対応機器が開発、販売されている。

[0081] このブルートゥースによる無線通信システムは、従来のIrDA(Infrared Data Association)のような赤外線通信方式と比較して、指向性がなく、透過性が高いなどの長所を有している。従って、IrDAなどの指向性が強い通信を利用する際には、通信を行わせる機器同士を適切に向かい合わせる必要があったが、ブルートゥースなどの通信システムでは、そのような位置の制約は不要となる。

[0082] ブルートゥースの規格に関しては、Bluetooth SIG Inc.によって管理されており、その詳細については、Bluetooth SIG Inc.から誰でも入手することが可能であるが、例えば、ブルートゥースを用いた通信においては、通信を制御するマスタと呼ばれる機器から、周囲に存在する機器を検出するための機器検出メッセージがブロードキャスト送信される。

[0083] そして、マスタは、この機器検出メッセージを受信した機器(スレーブ)から送信され

てきた応答メッセージによって、周囲に存在する機器、すなわち通信可能な機器を検出することができる。

[0084] また、マスタは、検出した機器の中から、特定の機器との間で通信を確立する場合、応答メッセージに含まれるそれぞれの機器の識別情報に基づいて機器を特定し、その通信を確立する。

[0085] ブルートゥースにおいては、そのような機器を識別する情報としてブルートゥースデバイス・アドレスと呼ばれる情報が個々の機器に付与されており、それぞれの機器に対して固有(一義的)であることから、機器の管理等、様々な処理に利用される。

[0086] 図7を参照して、ブルートゥース規格に準拠した無線通信ネットワークとしてのピコネットを形成して、ピコネットを形成した通信処理装置間で、相互に各種のデータを送受信する通信システムの構成例について説明する。

[0087] 前述したように、ブルートゥースを用いた通信においては、通信を制御するマスタと呼ばれる機器と、マスタを介した通信を実行する複数のスレーブと呼ばれる機器によって形成されるネットワーク(ピコネット)において通信が実行される。ブルートゥースにおいては、各機器を識別する情報としてブルートゥースデバイス・アドレスが個々の機器に設定され、ブルートゥースデバイス・アドレスに基づいて、通信対象の特定がなされる。

[0088] マスタとスレーブからなるピコネットにおいては、1つのマスタに対して、最大7つのスレーブが属することができる。同一のピコネットに属する全ての機器は、周波数軸(周波数ホッピングパターン)と時間軸(タイムスロット)が同期している状態にある。

[0089] 図7においては、パーソナルコンピュータ(PC)501がマスタとして設定され、その他の機器、パーソナルコンピュータ(PC)521、携帯電話522、PDA(Personal Digital Assistants)523、ビデオカメラ524が各々スレーブとして設定された構成例を示している。

[0090] これらの1つのマスタと複数のスレーブによって構成されるピコネットは、他の外部ネットワークと接続しない独立したネットワーク(アドホックモード)として存在することも、あるいはインターネット、あるいは他のピコネット等、他のネットワークにマスタを介して接続した構成(インフラストラクチャモード)とすることも可能である。

[0091] このピコネットは、パーソナルエリアネットワーク(PAN)とも呼ばれ、スレーブの各々は、PANU(PANユーザ:PAN User)と呼ばれる。また、他のネットワークと接続された構成(インフラストラクチャモード)におけるマスタは、ピコネットを構成するスレーブ間の通信パケットの中継、すなわちパケット交換処理を実行するとともに、外部接続ネットワークとのパケット交換も実行し、NAP(Network Access Point)と呼ばれる。一方、他の外部ネットワークと接続しない独立したネットワーク(アドホックモード)におけるマスタは、ピコネットを構成するスレーブ間の通信パケットの中継を行ない、GN(Group Ad-hoc Network)と呼ばれる。

[0092] ブルートゥースにおいては、無線通信で送受信されるデータや、その通信手順に関して、サービス毎に取り決めたプロファイルと呼ばれる仕様が策定されており、このプロファイルに従って、各機器が提供できるサービスが表わされている。PAN(Personal Area Network)プロファイルでは、ピコネットにおけるスレーブ間の通信方法が規定されており、PANプロファイルに基づいて構成されたピコネットに属する機器は、そのピコネットを1つのネットワークとして各種のデータを送受信する。

[0093] 図7に示すマスタとしてのパーソナルコンピュータ(PC)501、スレーブとしてのパーソナルコンピュータ(PC)521、携帯電話522、PDA523、ビデオカメラ524は、それぞれブルートゥースモジュールを内蔵しており、ブルートゥース規格に準拠した無線通信により、相互に各種のデータを送受信できるようになされている。

[0094] マスタ、スレーブを構成する各機器には、ブルートゥース規格に準拠した無線通信を実行するためのブルートゥースモジュールが備えられる。具体的には、無線周波数として、2.4GHzのISM帯を使用した時分割多重方式を採用し、ISM帯において周波数ホッピングスペクトラム拡散通信による無線通信を行なうためのモジュールである。

[0095] ブルートゥースモジュールの具体的構成例について、図8を参照して説明する。CPU601は、ROM602に格納されている制御プログラムをRAM603に展開し、ブルートゥースモジュール600の全体の動作を制御する。CPU601は、データ処理手段、あるいは通信制御処理手段として機能する。これらのCPU601乃至RAM603は、バス605を介して相互に接続されており、このバス605には、また、フラッシュメモリ604

が接続されている。

[0096] フラッシュメモリ604には、例えば、ピコネットを構成するマスタ、スレーブそれぞれのブルートゥースデバイスに設定されているブルートゥースデバイス名、および、それぞれのブルートゥースデバイスに対して固有なブルートゥースデバイス・アドレスなどが記憶されている。

[0097] このブルートゥースデバイス・アドレスは、48ビットの識別子であり、それぞれのブルートゥースデバイスに対して固有（一義的）であることから、ブルートゥースデバイスの管理に関する様々な処理に利用される。

[0098] 例えば、ピコネット内同期を確立するためには、全てのスレーブがマスタの周波数ホッピングパターンに関する情報を取得している必要があり、この周波数ホッピングパターンは、マスタのブルートゥースデバイス・アドレスに基づいてスレーブにより算出されるようになされている。

[0099] より詳細には、ブルートゥースデバイス・アドレスは、図9に示すように、24ビットのロー・アドレスパート（LAP：Low Address Part）と、8ビットのアッパー・アドレスパート（UAP：Upper Address Part）と、そして残りの16ビットのノンーシグニフィカントアドレスパート（NAP：Non-significant Address Part）とそれぞれ区分された構成を持ち、周波数ホッピングパターンの算出には、LAP全体の24ビットとUAPの下位4ビットからなる28ビットが用いられる。

[0100] スレーブの各々は、ピコネット内同期を確立するための「呼び出し（Page）」により取得したマスタのブルートゥースデバイス・アドレスの、上述した28ビットの部分と、同様にマスタから通知されたブルートゥースクロックに基づいて、周波数ホッピングパターンを算出することができる。

[0101] 図8の説明に戻る。フラッシュメモリ604には、ピコネット内同期確立後に、通信相手のブルートゥースデバイスを認証したり、送信するデータを暗号化したりするためのリンクキーなどが記憶され、必要に応じてCPU601に提供される。

[0102] 入出力インタフェース606は、CPU601からの指示に基づく供給データ、およびベースバンド制御部607から供給されてきたデータの入出力を管理する。

[0103] ベースバンド制御部607は、トランシーバ608の制御、リンクの制御、パケットの制

御、論理チャネルの制御、セキュリティの制御などの各種の制御、および誤り訂正符号化、復号化、或いはデータのランダム化などの処理を行い、入出力インタフェース606から供給されてきたデータをアナログ変換してトランシーバ608に出力するとともに、トランシーバ608から供給されてきた信号をデジタル変換して得られたデータを入出力インタフェース606に出力する。

[0104] トランシーバ608は、GFSK(Gaussian Frequency Shift Keying)変調部、GFSK復調部、スペクトラム拡散部、逆スペクトラム拡散部、或いはホッピングシンセサイザ部等より構成され、ベースバンド制御部607から供給されてきた信号に各種の処理を施し、アンテナ609に出力するとともに、アンテナ609から供給されてきた信号に各種の処理を施し、得られた信号をベースバンド制御部607に出力する。

[0105] トランシーバ608を構成するGFSK変調部は、ベースバンド制御部607から供給されてきたデータの高域成分をフィルタにより制限し、1次変調として周波数変調を行い、取得したデータをスペクトラム拡散部に出力する。スペクトラム拡散部は、上述したようにLAP全体の24ビットとUAPの下位4ビットからなる28ビットにより算出され、ホッピングシンセサイザ部から通知される周波数ホッピングパターンに基づいて搬送周波数を切り替え、供給されてきたデータに対してスペクトラム拡散を施した後に得られた信号をアンテナ609に出力する。ブルートゥースにおいては、スペクトラム拡散部は、625μ秒毎に周波数をホッピングさせて、データを送信するようになされている。

[0106] また、トランシーバ608を構成する逆スペクトラム拡散部は、ホッピングシンセサイザ部から通知される周波数ホッピングパターンに基づいて受信周波数をホッピングさせ、例えば、通信相手のスレーブから送信されてきた信号を取得する。また、逆スペクトラム拡散部は、取得した信号を逆スペクトラム拡散し、通信相手のスレーブからの信号を再生した後に得られた信号をGFSK復調部に出力する。GFSK復調部は、逆スペクトラム拡散部から供給されてきた信号をGFSK復調し、得られたデータをベースバンド制御部607に出力する。

[0107] トランシーバ608は、2．4GHz帯を使用して、スペクトラム拡散が施された信号をアンテナ609から送信する。また、トランシーバ608は、アンテナ609からの受信信号を逆スペクトラム拡散部に出力する。

[0108] なお、ピコネットを構成する通信処理装置の各々は、図8に示したブルートゥースモジュール600と同様の構成を有するモジュールを備えており、上述の処理により各装置各のデータ通信を実行する。

[0109] 上述したように、ブルートゥース規格に従った通信構成では、各機器はブルートゥースデバイス・アドレス(図9参照)という48ビットのIDを持つことが定められている。そして、このIDはブルートゥース規格に従った通信において、通信相手を特定するのに使用される。

[0110] 通常、ブルートゥースデバイス・アドレスの情報は、図8を参照して説明したように、ブルートゥースモジュールのICに直接つながる不揮発性メモリ(フラッシュメモリ604)に書き込まれており、ソフトウェアなどで読み出すことはできるが、変更することはできない。

[0111] 本実施例の認証シーケンスにおいては、ブルートゥースデバイス・アドレスを、2つの異なる方法で受信し、両者を比較して、一致すればローカル接続された機器間の通信、例えば同一のピコネットに接続された機器間の通信であると判定し、異なる場合には、外部ネットワークを介した通信であると判定する。

[0112] ブルートゥースデバイス・アドレスの取得処理は、以下の2つの取得処理によって取得したアドレスの比較を行う。

(1)通信相手のブルートゥースデバイス・アドレスの情報をピコネットを構築する際に取得する。

(2)例えば、2つの機器が共有する秘密鍵をもとにブルートゥースデバイス・アドレスを暗号化して伝送するプロトコルを決め、このプロトコルに従ってブルートゥースデバイス・アドレスを取得する。

[0113] このように、ピコネットを構築する際に取得した通信先デバイスのブルートゥースデバイス・アドレスと、アプリケーションレベルにおけるデータ処理によってパケットに格納したブルートゥースデバイス・アドレスまたはブルートゥースデバイス・アドレスに基づく2つのブルートゥースデバイス・アドレスを取得し、これらの照合を実行する。

[0114] 受信機器において、上記2つの方法で受信したブルートゥースデバイス・アドレスを比較して、一致すればローカル接続された機器間の通信、例えば同一のピコネットに

接続された機器間の通信であると判定し、異なる場合には、外部ネットワークを介した通信であると判定する。

[0115] ブルートゥース規格に従った通信を実行する機器同士で通信を行う場合、先に説明した図6(b)のように、機器A421と機器C422は秘密鍵を共有しており、機器X431が機器C422に、また機器Y432が機器A421になりすました場合、ブルートゥース通信範囲を超えた通信を行うことも可能である。これを防ぐため、機器A421はピコネット構築時に通信相手から取得したブルートゥースデバイス・アドレスと、前述の別のプロトコルによっても暗号などで保護されたブルートゥースデバイス・アドレスを取得する。

[0116] この場合、ピコネット構築時に通信相手から取得したブルートゥースデバイス・アドレスとしては、機器Xのブルートゥースデバイス・アドレスが設定されており、機器Aと秘密鍵を共有する機器は機器Cなので、機器X、Y経由で機器Cのブルートゥースデバイス・アドレスを取得することになる。そして、これらのブルートゥースデバイス・アドレスの照合により、不一致が判明すると、機器Cがブルートゥースによるローカル通信領域、例えば同一のピコネットに存在しないと判定し、外部ネットワークに中継された通信を停止し、コンテンツ流出等の秘密情報の漏洩を防止することができる。

[0117] (3)インターネットプロトコル規格に従った通信を行う構成例

次に、インターネットプロトコルに準拠したローカル通信を行う場合について述べる。一例として、イーサネットによりホーム・ネットワークが構築されている場合の例について説明する。

[0118] 現在、ホーム・ネットワークを構成するプロトコルとして、例えばUPnP(登録商標)が知られている。UPnPによれば、複雑な操作を伴うことなく容易にネットワークを構築することが可能であり、ネットワーク接続された機器間では困難な操作や設定を伴うことなくコンテンツ提供サービスを行なうことが可能となる。また、UPnPは、オペレーティング・システム(OS)に非依存であり、容易に機器の追加ができるという利点を持つ。

[0119] UPnPでは、ネットワーク接続された機器間で、XML(eXtensible Markup Language)形式で記述された定義ファイルを交換して相互認証を行なう。UPnPの処理

の概要は以下の通りである。

(1)アドレッシング処理:IPアドレスなどの自己のデバイスIDを取得する

(2)ディスカバリ処理:ネットワーク上の各デバイスの検索を行ない、各デバイスから受信した応答に含まれるデバイス種別や機能などの情報を取得する

(3)サービス要求処理:ディスカバリ処理で取得された情報に基づいて各デバイスにサービスを要求する

このような処理手順を行なうことで、ネットワーク接続された機器を適用したサービスの提供並びに受領が可能となる。新たにネットワークに接続される機器は、アドレッシング処理によりデバイスIDを取得し、ディスカバリ処理によりネットワーク接続されている他のデバイスの情報を取得し、サービス要求が可能となる。

[0120] ローカルバスであるホーム・ネットワークがイーサネットで構築されている場合、以下の2つの取得処理によって取得したMACアドレスの比較を行うことにより、認証相手機器がローカルネットワーク上に存在するか否かの判断を行う。

(1)ARP(Address Resolution Protocol)を用いて、IPアドレスからイーサネットの物理アドレス(MACアドレス)を求める。

(2)例えば、2つの機器が共有する秘密鍵をもとにMACアドレスを暗号化して伝送するプロトコルを決め、このプロトコルに従ってMACアドレスを取得する。

[0121] 図6(a)のように、機器A411と機器B412がローカルバスでつながっている場合の処理について、図10を参照して説明する。

[0122] ステップS301において、機器A411は機器B412のIPアドレスをARP問い合わせパケットに入れて、ネットワーク上にブロードキャストする。機器B412はARP問い合わせパケットを見ると、自分のIPアドレスが指定されているので、ARP応答パケットに自分のMACアドレスを入れて、応答を発信元である機器A411に返す(ステップS302)。ステップS301, S302の処理は、OSI参照モデルにおけるネットワーク層以下の処理として実行される。機器A411は受信した機器B412のMACアドレスをID1として保存する(ステップS303)。

[0123] IPネットワークにおいて暗号化されたコンテンツの伝送を行う際の、認証コマンドを拡張することにより、機器の認証処理部の間、つまりアプリケーションレイヤにおいて

、MACアドレスの問い合わせができるようにする。機器A411は、ステップS304において、MACアドレスの問い合わせのために拡張した認証コマンドを送信データとし、機器B412のIPアドレスを送信先としたIPパケットを送信する。機器B412はIPパケットを受信すると、アプリケーションレイヤである認証処理部において認証コマンドの処理をし、MACアドレスの問い合わせであると解釈する。そして、機器B412は、ステップS305において、認証コマンドの応答として自分のMACアドレスを機器A411に返送する。このステップS304，S305の処理はOSI参照モデルにおけるアプリケーション層の処理として実行される。

[0124] 機器A411は受信した機器B412のMACアドレスをID2として保存する。ステップS306において、機器A411はID1とID2との比較を実行し、これらの値が一致することから、機器A411と機器B412がローカルバスでつながっていると判断する。

[0125] 図6(b)のように実際には機器C422は機器A421と同じローカルネットワーク上には存在していないのに、機器X431、機器Y432を介して通信することにより、従来の認証シーケンスでは機器A421と機器C422のアプリケーションにおける認証が成立してしまう。本発明の構成では、これらの対応、すなわち、機器A421は、機器C422がローカルネットワーク接続機器でないことを判定することが可能となる。

[0126] 機器X431は機器C422のプロキシとして作用し、機器A421からはあたかも機器C422が機器X431の位置に存在する、つまり、ローカルネットワーク上に存在するように見える、という場合を想定する。機器A421はUPnPのディスカバリ処理において、ネットワーク上の各デバイスの検索を行ない、各デバイスから受信した応答に含まれるデバイス種別や機能などの情報を取得する。この応答において、機器X431は機器C422のデバイス種別・機能等の情報を自己の情報として返すのである。機器A421は、機器X431のIPアドレスを、機器C422のIPアドレスであると誤認識してしまう。機器A421は機器C422と認証を行うために、機器X431のIPアドレスを宛先として、IPパケットを送信する。機器X431はパケットを受信すると、これを機器C422宛てのパケットに書き換え、機器Y432を介して機器C422に送信する。

[0127] 図11を参照して、機器A421によって、機器C422がローカルネットワークに存在するかを判定する処理シーケンスについて説明する。

[0128] 機器C422がローカルネットワークに存在するかの判断のため、機器A421は、ステップS401において、機器C422のIPアドレス(実際には機器X431のIPアドレス)をARP問い合わせパケットに入れて、ネットワーク上にブロードキャストする。機器X431はARP問い合わせパケットを見ると、自分のIPアドレスが指定されているので、ARP応答パケットに自分のMACアドレスを入れて、応答を発信元である機器A421に返す(ステップS402)。ステップS401, S402の処理は、OSI参照モデルにおけるネットワーク層以下の処理として実行される。ステップS403において、機器A421は受信した機器X431のMACアドレスをID1として保存する。

[0129] 次に、機器A421は、ステップS404において、MACアドレスの問い合わせのために拡張した認証コマンドを送信データとし、機器X431のIPアドレスを送信先としたIPパケットを送信する。機器X431はIPパケットを受信すると、機器C422宛てパケットとして、機器Y432を介して機器C422に送信する。機器C422はIPパケットを受信すると、アプリケーションレイヤである認証処理部において認証コマンドの処理をし、MACアドレスの問い合わせであると解釈する。そして、機器C422は、ステップS405において、認証コマンドの応答として自分のMACアドレスを機器A421に返送する。

[0130] 機器A421は受信した機器C422のMACアドレスをID2として保存する。ステップS406において、機器A421はID1とID2との比較を実行し、これらの値が一致しないことから、機器C422が、機器A421の接続されたローカルネットワーク上に存在しないと判断する。

[0131] 上述したように、本発明の構成によれば、ホーム・ネットワーク等のネットワークに対して、インターネット等の外部ネットワークに接続された機器からアクセスされた場合、そのアクセスが外部機器からか内部のローカルネットワーク内の機器からであるかを明確に判別することが可能となり、ローカルネットワーク内の秘密情報、例えば私的データや、著作権、利用権の制限されたコンテンツの漏洩、流出を未然に防止することが可能となる。

[0132] 以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的

に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

[0133] なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

[0134] 例えば、プログラムは記録媒体としてのハードディスクやROM(Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD-ROM(Compact Disc Read Only Memory), MO(Magneto optical)ディスク, DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納(記録)しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

[0135] なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

[0136] なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

産業上の利用可能性

[0137] 以上、説明したように、本発明の構成によれば、ホーム・ネットワーク等のネットワークに対して、インターネット等の外部ネットワークに接続された機器からアクセスされた場合、そのアクセスが外部機器からか内部のローカルネットワーク内の機器からであるかを明確に判別することが可能となり、ローカルネットワーク内の秘密情報、例えば

私的データや、著作権、利用権の制限されたコンテンツの漏洩、流出を未然に防止することが可能となり、コンテンツ著作権の管理の必要なコンテンツや、私的コンテンツ等、漏洩を防止することが必要なデータをローカルネットワーク内でのみ利用しようとするシステムにおいて適用されるデバイスで実行する認証シーケンスとしての適用が可能である。

図面の簡単な説明

[0138] [図1]ネットワーク構成例について説明する図である。

[図2]通信処理装置の構成について説明する図である。

[図3]IEEE1394機器の構成について説明する図である。

[図4]本発明の認証シーケンスについて説明するフロー図である。

[図5]本発明の認証シーケンスについて説明するシーケンス図である。

[図6]本発明の認証シーケンスによるID取得処理および効果について説明する図である。

[図7]ブルートゥース規格による通信ネットワークについて説明する図である。

[図8]ブルートゥースデバイスの構成について説明する図である。

[図9]ブルートゥースデバイスの通信において適用されるブルートゥースデバイス・アドレスの構成について説明する図である。

[図10]インターネットプロトコルに準拠した通信において、本発明に基づく機器判定処理を実行した場合の通信シーケンスを説明する図である。

[図11]インターネットプロトコルに準拠した通信において、本発明に基づく機器判定処理を実行した場合の通信シーケンスを説明する図である。

符号の説明

[0139] 100 ホーム・ネットワーク

101 PC

102 PC

103 TV

104 ハードディスクレコーダ

105 PDA

120 外部ネットワーク

121 PC

122 携帯電話

123 ポータブル再生プレーヤ

201 CPU(Central Processing Unit)

202 ROM(Read Only Memory)

203 RAM(Random Access Memory)

204 HDD(Hard Disk Drive)

205 バス

206 入出力インタフェース

207 入力部

208 出力部

209 通信部

210 ドライブ

211 リムーバブル記録媒体

301 送受信部

302 IEEE1394端子

303 PHY-IC(PHY通信部)

304 LINK-IC

305 ネットワーク通信部(IEEE1394制御マイコン)

306 機器制御マイコン

310 1394バス

411 機器A

412 機器B

421 機器A

422 機器C

431 機器X

501 パーソナルコンピュータ(PC)

521 パーソナルコンピュータ(PC)

522 携帯電話

523 PDA(Personal Digital Assistants)

524 ビデオカメラ

600 ブルートゥースモジュール

601 CPU

602 ROM

603 RAM

604 フラッシュメモリ

605 バス

606 入出力インタフェース

607 ベースバンド制御部

608 トランシーバ

609 アンテナ

請求の範囲

[1] ネットワークを介した通信処理を実行する通信処理装置であり、

所定の認証方式に対応したローカルネットワーク内の機器にのみ開示が許可されている秘密情報を取得するため、前記認証方式による認証処理に関連した通信処理を行い、

OSI参照モデルにおけるネットワーク層以下のデータ処理によって、前記通信処理における通信先デバイスの固有識別情報を取得し、

OSI参照モデルにおけるアプリケーション層のデータ処理として、前記認証方式の認証シーケンスにて、認証相手デバイスの固有識別情報を取得し、

取得した、前記通信先デバイスの固有識別情報識別情報と、前記認証相手デバイスの固有識別情報との照合を行い、

該照合の成立または非成立に基づいて、認証相手デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する構成を有することを特徴とする通信処理装置。

[2] 通信先デバイスから受信する少なくとも1つの固有識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成処理によって生成した処理データとして受信する構成であることを特徴とする請求項1に記載の通信処理装置。

[3] 通信先デバイスから受信する識別情報は、IEEE1394規格によって規定されたノードユニークIDであることを特徴とする請求項1に記載の通信処理装置。

[4] 前記通信処理装置は、

通信先デバイスから受信する識別情報として、通信先デバイスのPHY通信部の取得した識別情報と、通信先デバイスのネットワーク通信部の取得した識別情報とを受信し、これらの複数の識別情報の照合を行う構成であることを特徴とする請求項1に記載の通信処理装置。

[5] 通信先デバイスから受信する識別情報は、通信規格によって規定されたデバイス・アドレスであることを特徴とする請求項1に記載の通信処理装置。

[6] 前記通信処理装置は、

通信先デバイスから受信する識別情報として、通信先デバイスの送信するパケットのソースアドレスとしてのデバイス・アドレスと、アプリケーションレベルにおけるデータ処理によってパケットに格納したデバイス・アドレスまたはデバイス・アドレスに基づくデータを受信し、これらの複数のデバイス・アドレスの照合を行う構成であることを特徴とする請求項1に記載の通信処理装置。

[7] ネットワークを介した通信処理を実行する通信制御方法であり、

OSI参照モデルにおけるネットワーク層以下のデータ処理によって、通信処理における通信先デバイスの固有識別情報を取得し、OSI参照モデルにおけるアプリケーション層のデータ処理として、所定の認証方式の認証シーケンスにて、認証相手デバイスの固有識別情報を取得する識別情報取得ステップと、

取得した、前記通信先デバイスの固有識別情報識別情報と、前記認証相手デバイスの固有識別情報との照合を実行する照合処理ステップと、

該照合の成立または非成立に基づいて、認証相手デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する判定ステップと、

を有することを特徴とする通信制御方法。

[8] 前記識別情報取得ステップにおいて通信先デバイスから受信する少なくとも1つの固有識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成処理によって生成した処理データとして受信することを特徴とする請求項7に記載の通信制御方法。

[9] 通信先デバイスから受信する識別情報は、IEEE1394規格によって規定されたノードユニークIDであることを特徴とする請求項7に記載の通信制御方法。

[10] 前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、通信先デバイスのPHY通信部の取得した識別情報と、通信先デバイスのネットワーク通信部の取得した識別情報とを受信するステップであり、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする請求項7に記載の通信制御方法。

[11] 通信先デバイスから受信する識別情報は、通信規格によって規定されたデバイス・アドレスであることを特徴とする請求項7に記載の通信制御方法。

[12] 前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、通信先デバイスの送信するパケットのソースアドレスとしてのデバイス・アドレスと、アプリケーションレベルにおけるデータ処理によってパケットに格納したデバイス・アドレスまたはデバイス・アドレスに基づくデータを受信し、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする請求項7に記載の通信制御方法。

[13] ネットワークを介した通信処理を実行するコンピュータ・プログラムであり、

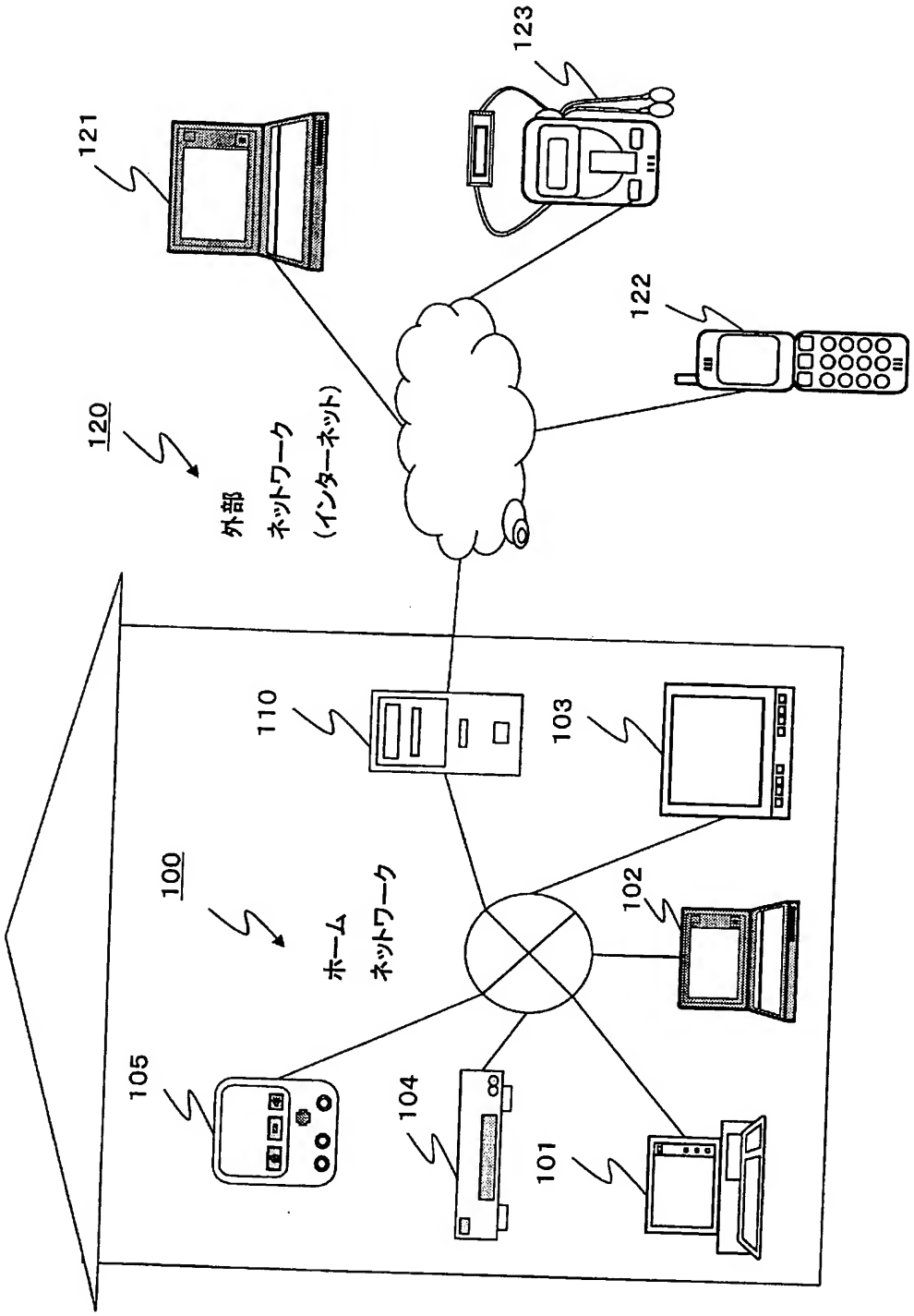
OSI参照モデルにおけるネットワーク層以下のデータ処理によって、通信処理における通信先デバイスの固有識別情報を取得し、OSI参照モデルにおけるアプリケーション層のデータ処理として、所定の認証方式の認証シーケンスにて、認証相手デバイスの固有識別情報を取得する識別情報取得ステップと、

取得した、前記通信先デバイスの固有識別情報識別情報と、前記認証相手デバイスの固有識別情報との照合を実行する照合処理ステップと、

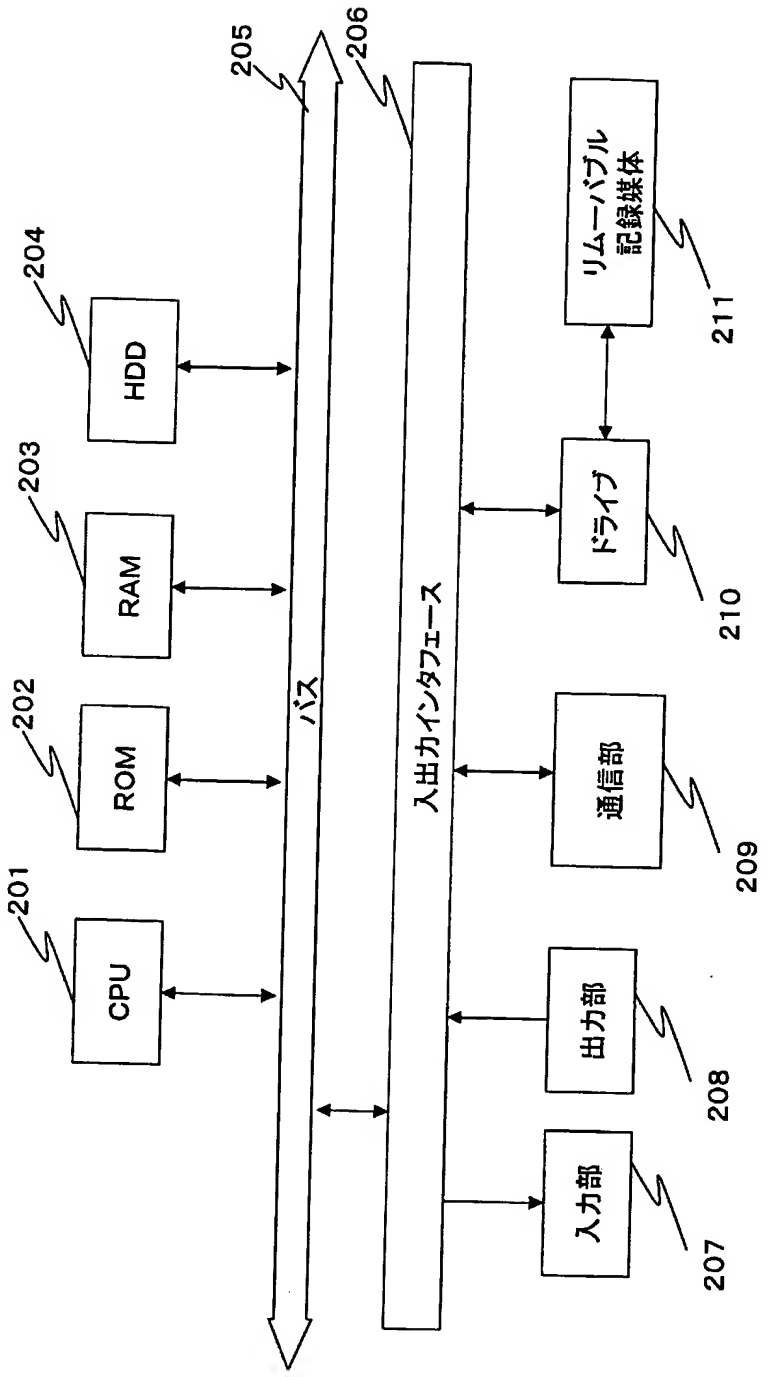
該照合の成立または非成立に基づいて、認証相手デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する判定ステップと、

を有することを特徴とするコンピュータ・プログラム。

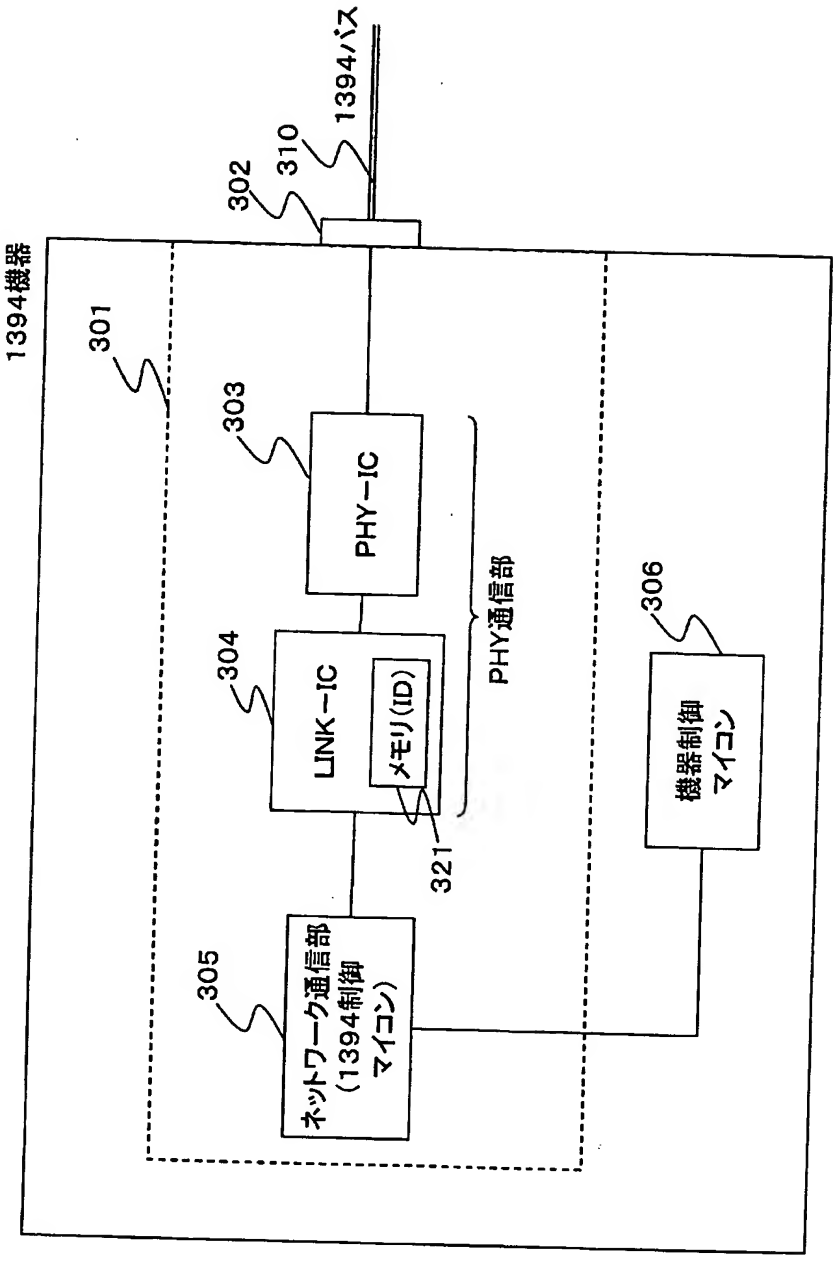
[図1]


123
121
122
120
外部
ネットワーク
(インターネット)
110
103
100
ホーム
ネットワーク
102
105
104
101

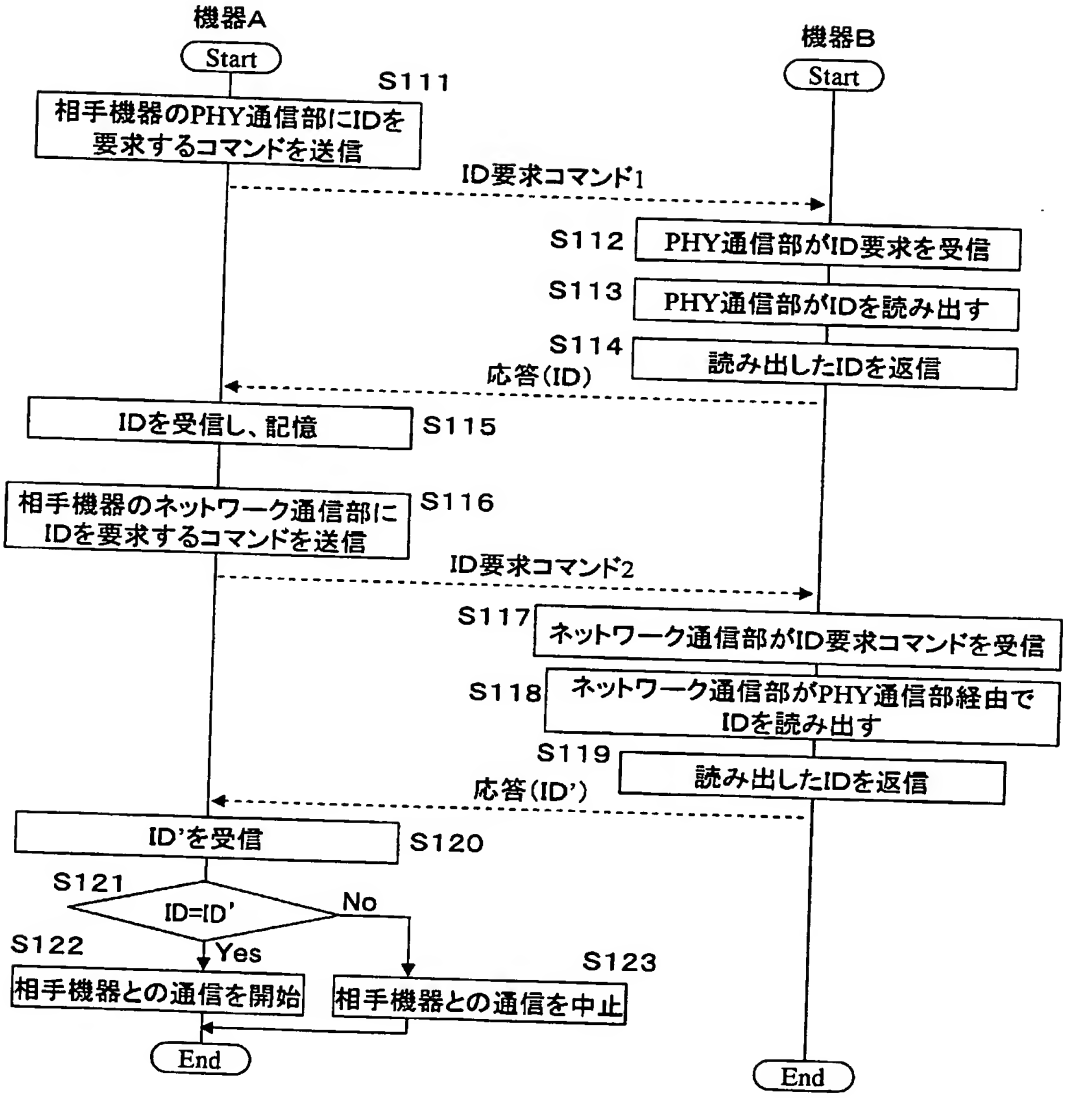
[図2]


205
206
204
HDD
203
RAM
202
ROM
201
CPU
バス
入出力インタフェース
リムーバブル記録媒体
211
ドライブ
210
通信部
209
出力部
208
入力部
207

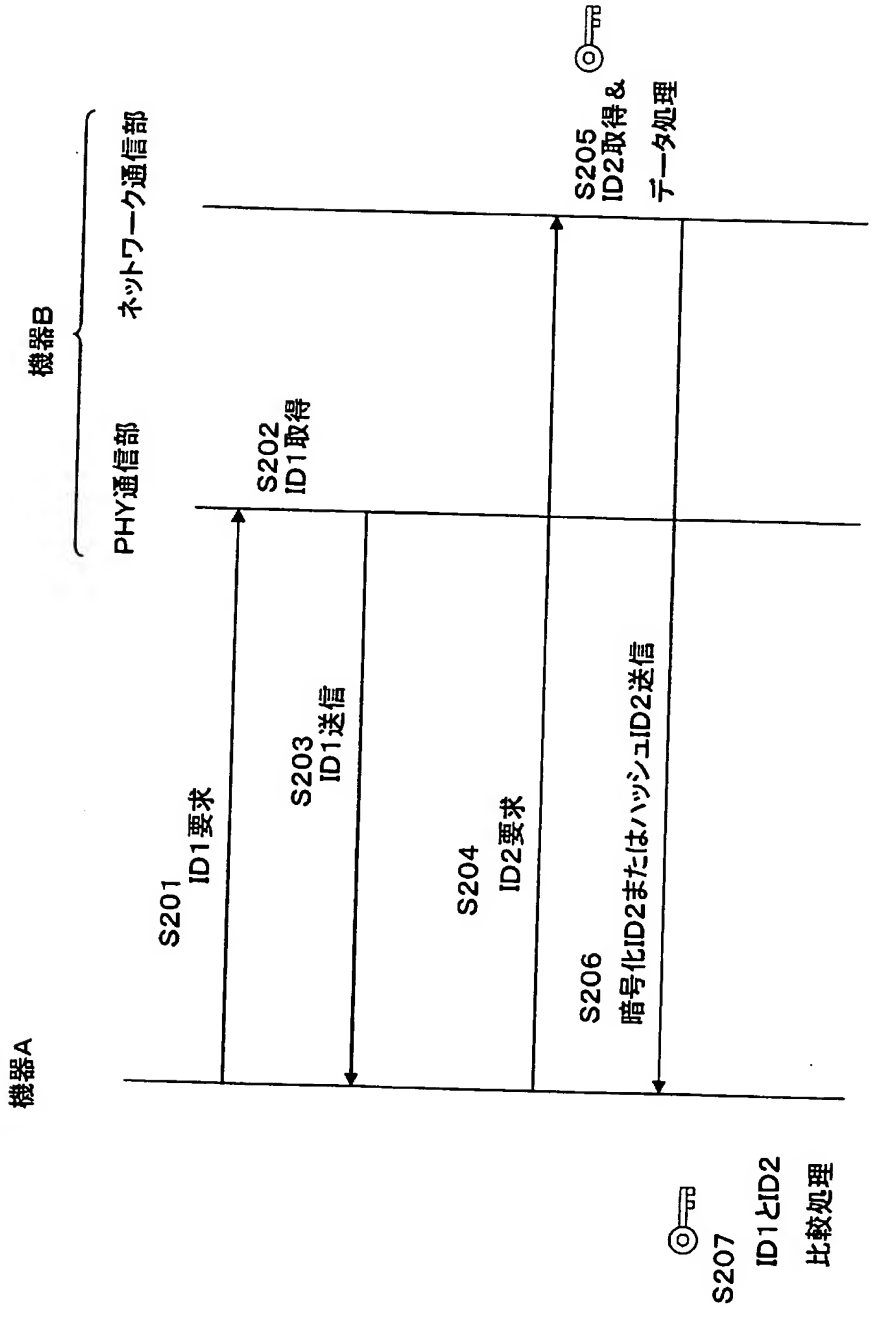
[図3]


1394バス
310
302
1394機器
301
303
PHY−IC
304
LINK−IC
メモリ(ID)
PHY通信部
306
機器制御
マイコン
321
305
ネットワーク通信部
(1394制御
マイコン)

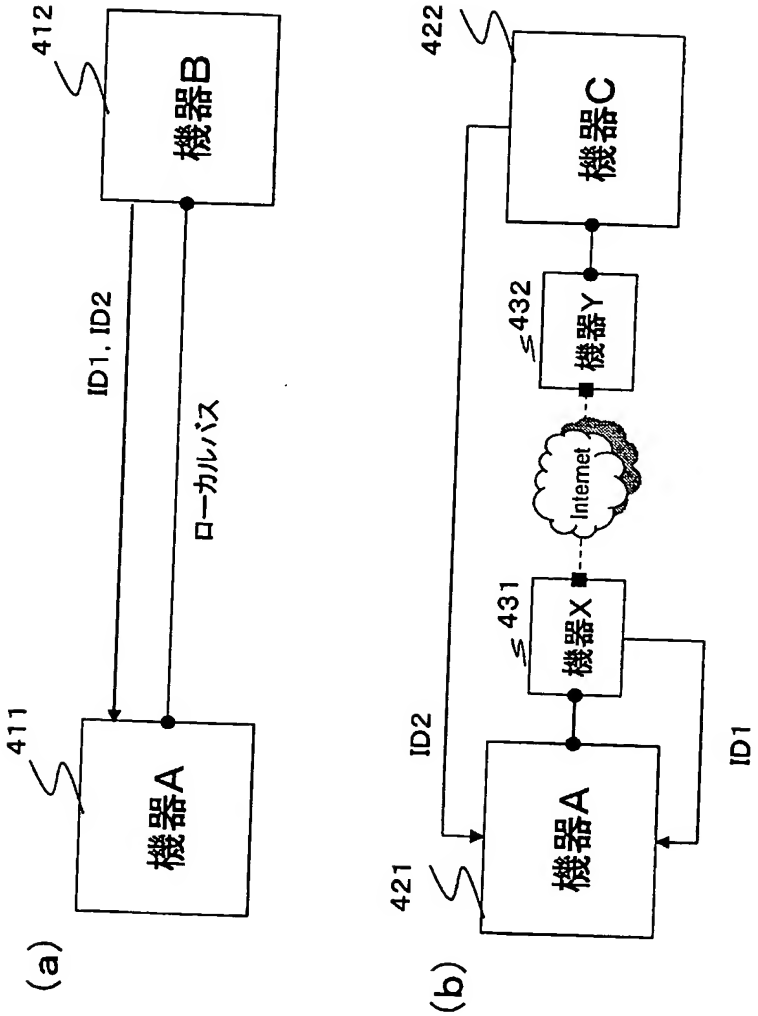
[図4]


機器A
Start
S111
相手機器のPHY通信部にIDを要求するコマンドを送信
ID要求コマンド1
機器B
Start
S112
PHY通信部がID要求を受信
S113
PHY通信部がIDを読み出す
S114
読み出したIDを返信
応答(ID)
IDを受信し、記憶
S115
相手機器のネットワーク通信部にIDを要求するコマンドを送信
S116
ID要求コマンド2
S117
ネットワーク通信部がID要求コマンドを受信
S118
ネットワーク通信部がPHY通信部経由でIDを読み出す
S119
読み出したIDを返信
応答(ID')
ID'を受信
S120
S121
ID=ID'
No
Yes
S122
相手機器との通信を開始
S123
相手機器との通信を中止
End
End

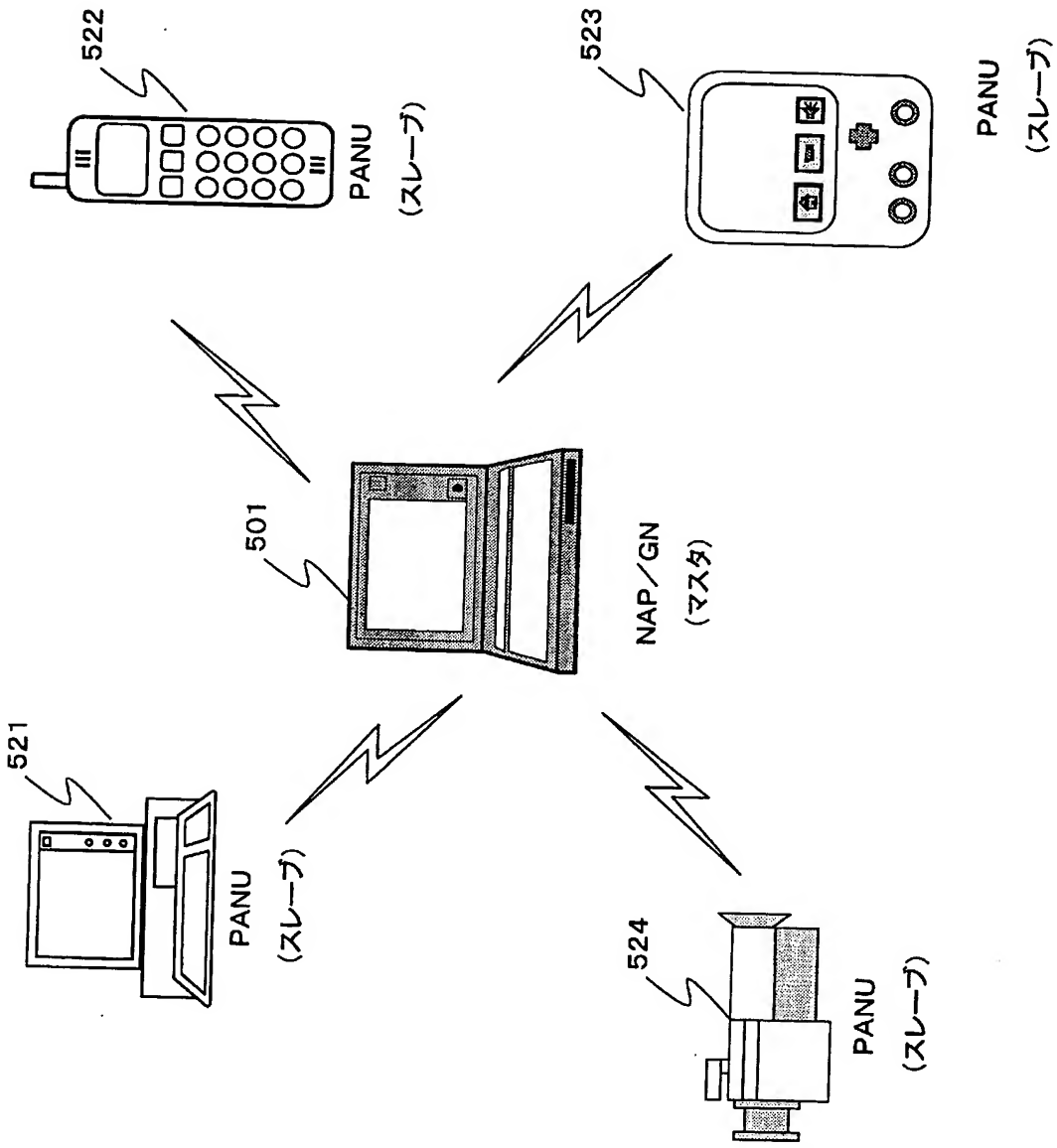
[図5]


機器A
機器B
PHY通信部
ネットワーク通信部
S201
ID1要求
S202
ID1取得
S203
ID1送信
S204
ID2要求
S205
ID2取得&
データ処理
S206
暗号化ID2またはハッシュID2送信
S207
ID1とID2
比較処理

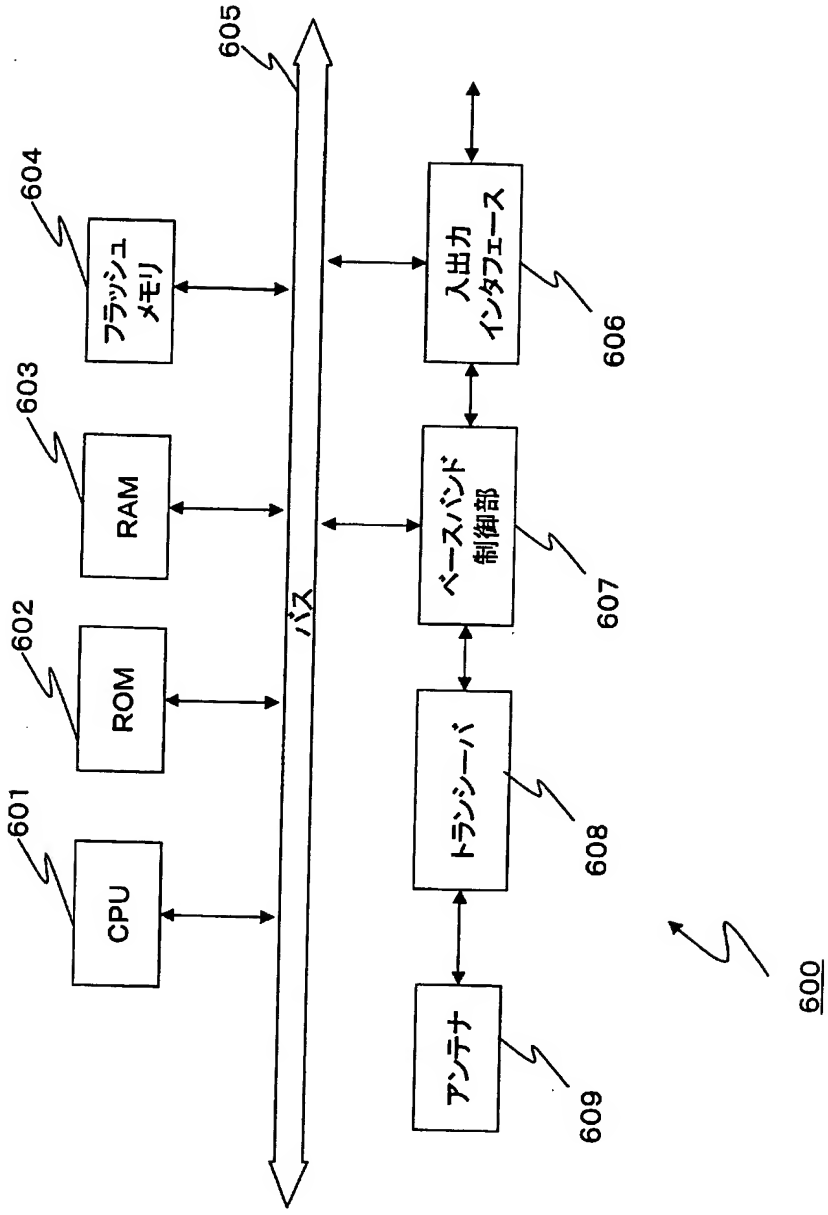
[図6]


412
機器B
ID1, ID2
ローカルバス
411
機器A
(a)
422
機器C
432
機器Y
Internet
431
機器X
ID2
ID1
421
機器A
(b)

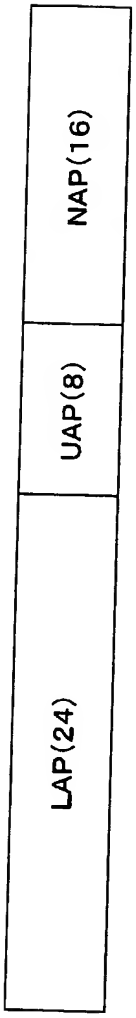
[図7]


522
PANU
(スレーブ)
523
PANU
(スレーブ)
501
NAP/GN
(マスタ)
521
PANU
(スレーブ)
524
PANU
(スレーブ)

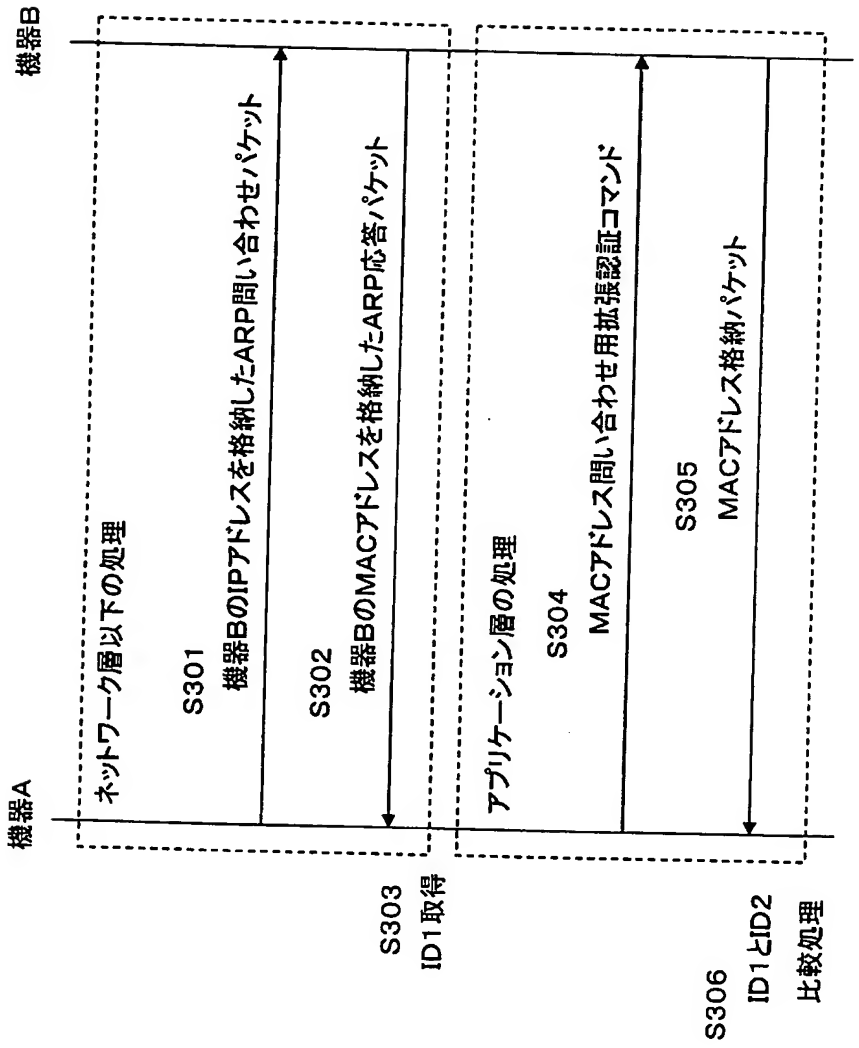
[図8]


605
604
フラッシュメモリ
603
RAM
602
ROM
601
CPU
バス
入出力インタフェース
606
ベースバンド制御部
607
トランシーバ
608
アンテナ
609
600

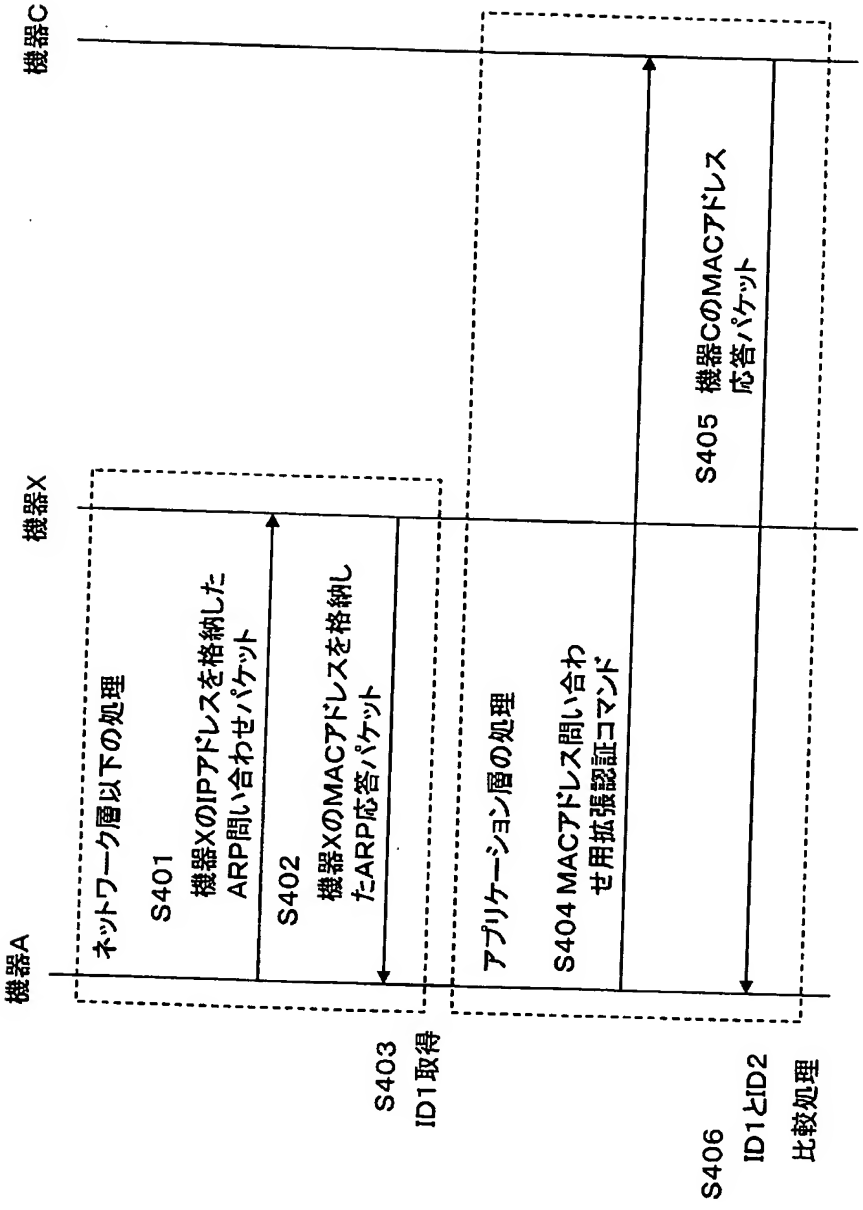
[図9]



[図10]


機器B
機器A
ネットワーク層以下の処理
S301
機器BのIPアドレスを格納したARP問い合わせパケット
S302
機器BのMACアドレスを格納したARP応答パケット
S303
ID1取得
アプリケーション層の処理
S304
MACアドレス問い合わせ用拡張認証コマンド
S305
MACアドレス格納パケット
S306
ID1とID2
比較処理

[図11]


機器A
機器X
機器C
ネットワーク層以下の処理
S401
機器XのIPアドレスを格納したARP問い合わせパケット
S402
機器XのMACアドレスを格納したARP応答パケット
S403
ID1取得
アプリケーション層の処理
S404 MACアドレス問い合わせ用拡張認証コマンド
S405 機器CのMACアドレス応答パケット
S406
ID1とID2比較処理

国際調査報告

国際出願番号　PCT／JP2004／011475

A.　発明の属する分野の分類（国際特許分類（IPC））
Int. Cl⁷ H04L12／28, G06F15／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））
Int. Cl⁷ H04L12／28, G06F15／00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2004年
日本国登録実用新案公報　1994－2004年
日本国実用新案登録公報　1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 2001－285284 A（株式会社東芝）2001.10.12, 全文（ファミリーなし）	1－13
A	JP 10－149338 A（株式会社アイ・オー・データ機器）1998.06.02, 全文（ファミリーなし）	1, 2, 4－8, 10－13
A	JP 2000－201143 A（日本電気株式会社）2000.07.18, 全文（ファミリーなし）	1, 2, 4－8, 10－13

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 26.10.2004	国際調査報告の発送日 09.11.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 中木　努　5X　3464 電話番号　03－3581－1101　内線　3556

様式PCT／ISA／210（第2ページ）（2004年1月）

国際調査報告

国際出願番号　PCT／JP2004／011475

C（続き）　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 2002－222172 A（日本電信電話株式会社）2002．08．09，段落番号【0009】～【0017】（ファミリーなし）	1，2，4－8，10－13